IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION Plaintiff, vs. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity, Defendant.	C.A. No. 1:20-cv-12090-DPW **PUBLIC REDACTED VERSION**

Revised Affidavit of Kevin Tierney

1. My name is Kevin Tierney. I am 40 years old and reside in Brighton, Michigan.

2. Since 2019, I have been the Vice President of Global Cybersecurity at General Motors Company ("GM"), responsible for overseeing GM's global cybersecurity program. I have been employed by GM for a total of fifteen years, the last seven in cybersecurity. This affidavit is based on my personal knowledge.

3. GM is one of the largest automakers in the world. In 2020, GM shipped approximately seven million vehicles globally, with about 2.5 million vehicles sold in the United States. GM currently has sixty dealerships in Massachusetts. In 2020, GM delivered 29,516 vehicles to Massachusetts.

4. GM is a member of the plaintiff trade association, the Alliance for Automotive Innovation ("Auto Innovators").

Overview

5. GM manufactures numerous models of vehicles, including Chevrolet, Cadillac, GMC, and Buick. GM distributes a large number of new automobiles it manufactures to

independently owned GM-affiliated dealerships in the Commonwealth of Massachusetts for initial sale to consumers.

6. GM equips the vast majority of its vehicles for individual sale with telematics systems. Telematics is a radio-enabled system that allows remote communication with vehicles and supports several vehicle features including in-vehicle GPS navigation systems, emergency response, remote starting, and firmware over-the-air (FOTA) updates to vehicles. FOTA allows for remote updating of vehicle software, including software that addresses recall and safety concerns. For over a decade, GM has sold vehicles in Massachusetts equipped with GM's telematics system, called OnStar.

7. Model year 2022 vehicles are currently in production and will be shipping soon. GM completed the design and validation process for model year 2022 vehicles prior to November 2020—that is, before Massachusetts voters passed the ballot initiative at issue in this case (the "Data Law") and well before the law became effective.

8. GM completed the design and testing of its model year 2022 vehicles over several years. The electrical architecture design for model year 2022 vehicles was completed between April 2017 and June 2019, depending on the vehicle model.

9. GM follows a very detailed and stringent product development process that requires extensive testing for federal and state regulatory compliance, product assurance, consumer preference, cybersecurity, and product safety. This process includes adherence to GM's policy of maintaining a secure development lifecycle. That policy requires GM to consider cybersecurity throughout all phases of development (commonly referred to as "security by design"). As a result, the GM teams responsible for vehicle cybersecurity work in lockstep with the GM teams developing all aspects of the vehicle, including ensuring cybersecurity protections around safety-

critical vehicle functions like acceleration, braking, steering, and airbag deployment. Attached hereto as Trial Exhibit 36 is a true and correct copy of GM's security by design policy (AAI-GM-0000022).

10. When implementing new technology in vehicles, GM typically deploys updates over several model years. For example, when GM creates a new version of its OnStar system, the new system is not implemented in all vehicles across one model year.

11. A dedicated team of specialists working in GM's Product Cybersecurity Group design and maintain GM's cybersecurity controls. That team is a large, global organization of more than seventy-five people responsible for ensuring the safety, security, and privacy of GM's customers across all brands and global regions. The team comprises specialists including security engineers, architects, analysts, data scientists, and security testers.

12. GM's multi-year product development process makes it impossible for GM to develop and implement the considerable changes to vehicle architecture required by the Data Law. Even if such a system were possible while ensuring the safe operation of GM vehicles, development would have needed to start years ago for GM to have sufficient time to develop, test, validate, and deploy such a system across all brands and models immediately.

13. More importantly, as I discuss in detail later, the Data Law's requirements run directly counter to GM's cybersecurity approach, and would seriously compromise vehicle safety and emissions control. They would force GM to remove existing cybersecurity controls around safety- and emissions-critical functions. Rather than offering consumers greater protection, removing existing cybersecurity controls would leave vehicles more vulnerable to cyberattack and increase the potential severity of any cyberattack.

NHTSA and Vehicle Safety

14. The National Highway Traffic Safety Administration ("NHTSA") regulates the safety of motor vehicles and related equipment. NHTSA has the authority to direct recalls of vehicles that pose an unreasonable safety risk or do not meet federal safety standards. NHTSA has stated that this authority includes the ability to force a manufacturer to engage in expensive recall efforts for deficient cybersecurity around vehicle safety systems.

15. NHTSA promotes its safety policy and objectives in part through recalls. Most recalls are done voluntarily and proactively by the manufacturers. *See, e.g.*, NHTSA, *2020 Recall Annual Report* 2, https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/2020_nhtsa_recall_annual_report_021021-tag.pdf (noting that only 38 out of 786 recalls in 2020 were influenced by NHTSA), a true and correct copy of which is attached hereto as Trial Exhibit 37.

16. Manufacturers also have an obligation to try to prevent unreasonable safety risks by undertaking safety recalls, if necessary, and notifying NHTSA of the issue and the recall. In practice, most recalls are "voluntary" in the sense that the manufacturer initiates and runs the process without being told to do so by NHTSA, as required under federal law. Despite this cooperative approach, at the end of the day, NHTSA retains the right to order manufacturer recalls.

17. NHTSA and manufacturers communicate regularly regarding safety issues. GM has met with NHTSA on multiple occasions to describe its approach to vehicle cybersecurity and demonstrate GM's efforts to safeguard safety-related systems from cybersecurity risks. Attached hereto as Trial Exhibit 38 is a true and correct copy of GM's July 2019 presentation entitled *Global Cybersecurity* for a NHTSA meeting (AAI-GM-0000056). Attached hereto as Trial Exhibit 15 is a true and correct copy of GM's May 2020 presentation entitled *Global Cybersecurity* for a

NHTSA meeting (AAI-GM-0001065). Both of these presentations were prepared by me and my team at GM.

18. NHTSA also issues guidance on several issues in the automotive industry. Cybersecurity is no exception. In 2016, NHTSA published Cybersecurity Best Practices for the Safety of Modern Vehicles, which guides the automotive industry for improving vehicle cybersecurity for safety. GM takes guidance from NHTSA seriously, in part to avoid costly recalls.

19. NHTSA recommends, among other protections, using a "layered approach," using encryption, restricting the ability to change a vehicle's firmware, and segmenting different functions (logical and physical isolation). *See* NHTSA, *Cybersecurity Best Practices for the Safety of Modern Vehicles* (2016), www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf ("NHTSA Cybersecurity Best Practices"). Just last year, NHTSA reaffirmed these principles. *See* NHTSA, *Cybersecurity Best Practices for the Safety of Modern Vehicles Draft 2020 Update* (2020), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf; *see also Request for Comments on NHTSA's Cybersecurity Best Practices for the Safety of Motor Vehicles Draft 2020 Update*, 86 Fed. Reg. 2481, 2481 (Jan. 12, 2021) ("motor vehicle cybersecurity remains a top priority for NHTSA"). Attached hereto as Trial Exhibits 3 and 24 are true and correct copies of NHTSA's 2016 and 2020 cybersecurity best practices, respectively.

20. As discussed below, GM has built security layers and protocols into the design of its safety systems consistent with NHTSA best practices and manufacturers' federal regulatory obligations. GM adheres to NHTSA best practices to help to ensure that its vehicles stay in safe condition, avoid unreasonable safety risks, and avoid recalls. GM continues to update its cybersecurity controls as new safety issues or concerns emerge.

21. Maintaining sufficient cybersecurity controls in line with NHTSA's recommendation is not optional. GM is well aware of the 2015 cybersecurity-related recall that FCA instituted in coordination with NHTSA when it was determined that threat actors could potentially exploit a weakness in cybersecurity controls around radio functions and take command of vehicles. The 2015 FCA recall shows that NHTSA considers cybersecurity vulnerabilities to be an unreasonable safety condition implicating a manufacturer's recall obligations.

22. NHTSA also promulgates Federal Motor Vehicle Safety Standards ("FMVSS"), compliance with which is binding on auto manufacturers. These FMVSSs cover safety-critical functions such as accelerator control systems, 49 C.F.R. § 571.124, electronic stability control ("ESC") systems for steering and anti-lock braking, *id.* § 571.126; light-vehicle braking, *id.* § 571.135; and occupant crash protection such as airbags, *id.* § 571.208.

23. The FMVSS for accelerator control systems, ESC, and light vehicle braking were drafted with the intention that there would be a driver present and in control of the systems when the vehicle is in operation.

24. If a threat actor controls a vehicle's acceleration, rather than the driver, the accelerator control system will not function as intended, which could jeopardize the safety of the system.

25. Similarly, if a threat actor—or malware introduced by a threat actor—could change the timing of deployment of a vehicle's airbags, that would directly implicate the safety of the driver and other occupants of a vehicle, all of which are regulated by federal law. Manufacturers, vehicle dealers, distributors, and others are prohibited from removing or disabling any part or design elements of a federally-mandated safety system in a motor vehicle.

26. GM installed the cybersecurity controls described below to protect (among others) safety-critical functions like acceleration, braking, steering, and airbag deployment. Those cybersecurity controls are a key part of the design element and safety systems of GM vehicles. GM is prohibited from rendering these controls inoperative and thus opening up regulated safety-critical systems to greater cybersecurity risk.

EPA and the Clean Air Act

27. The Clean Air Act, and Environmental Protection Agency ("EPA") regulations promulgated under that Act, require that all vehicles that GM sells in the United States comply with federal emissions requirements. Those emissions obligations extend for the useful life of the vehicle.

28. The Clean Air Act prohibits tampering with emissions control software. To comply with the Clean Air Act and EPA's regulations, GM includes as part of the design element of its vehicles cybersecurity controls around emissions-related ECUs like the engine control module. These are designed to prevent manipulation of the vehicle's systems that might increase emissions. That manipulation may come from third-parties or the vehicle owner him- or herself, who might desire to modify vehicle performance at the cost of higher vehicle emissions.

29. The Clean Air Act forbids GM from removing design elements installed to comply with EPA emissions requirements.

Background on Modern Vehicles

30. Modern vehicles comprise large, complex computer systems that control nearly every aspect of a vehicle's functionality.

31. Vehicles contain a myriad of electronic control units ("ECUs") that execute vehicle functions. ECUs control everything from convenience features like climate control and keyless

entry to safety-critical functions like acceleration and steering—and everything in between (such as, for instance, opening and closing windows).

32. GM has individual ECUs for systems such as vehicle accelerator controls, transmission controls, steering controls, ABS, and airbag deployment.

33. Sensors measuring conditions throughout the vehicle support the ECUs. For example, sensors attached to the vehicle's wheels and crankshaft measure speed and communicate this information to the ECU that manages fuel injection in the engine.

34. These ECUs and sensors communicate with each other via the "busses" in the vehicle's networks—principally on Controller Area Network ("CAN") busses. By design, not all busses communicate directly with each other. That is especially true of those busses that contain safety-critical ECUs. Instead, a central gateway module allows limited communications between busses and monitors the network traffic for any malicious or unauthorized messages.

35. The growth of infotainment such as radio and integration with a driver's mobile device and other connectivity features have further fueled the complexity of vehicles' electronic components, introducing new external-facing wired and wireless vehicle interfaces.

36. Telematics systems provide drivers with desirable features such as GPS and hands-free calling while facilitating safety functions. But they also promote vehicle safety. For example, telematics enables FOTA updates that allow manufacturers to update important safety features without the vehicle returning to a dealership or repair shop. Telematics also enables emergency services through OnStar, which allows for remote support if a vehicle is in an accident.

37. Telematics systems do not, however, provide manufacturer-affiliated dealerships or independent repair shops with vehicle diagnostic, repair, and maintenance data. The type of

data used to conduct traditional vehicle repairs flows instead through vehicle on-board diagnostic ("OBD") ports, discussed in more detail below.

38. The increasingly electronic nature of vehicles has also introduced new challenges for vehicle security as, for instance, external connections expand the vehicle's attack surface. An attack surface refers to all the access points that could allow for a threat actor to gain access. Attack surfaces increase the more access points are available in a system. Threat actors can access vehicles remotely via wireless networks. *See* Presentation entitled *Vehicle Cybersecurity Overview* (AAI-GM-0000011), a true and correct copy of which is attached hereto as Trial Exhibit 39, which was prepared by me and my team at GM in 2015.

39. Since 1996, EPA has required second-generation on-board diagnostic ("OBD") systems, OBD-II, to monitor emissions systems. Manufacturers, including GM, now also use OBD software to monitor other non-emissions systems. The OBD system uses a standard set of diagnostic codes that technicians, both at dealerships and independent repair shops, access through an OBD tool or scan tool. Technicians do not need manufacturer authorization to access many OBD diagnostic codes. But that access is limited. For instance, technicians must have manufacturer authorization before they can modify or update ECU software on the OBD system. The software used to make those updates is manufacturer-specific.

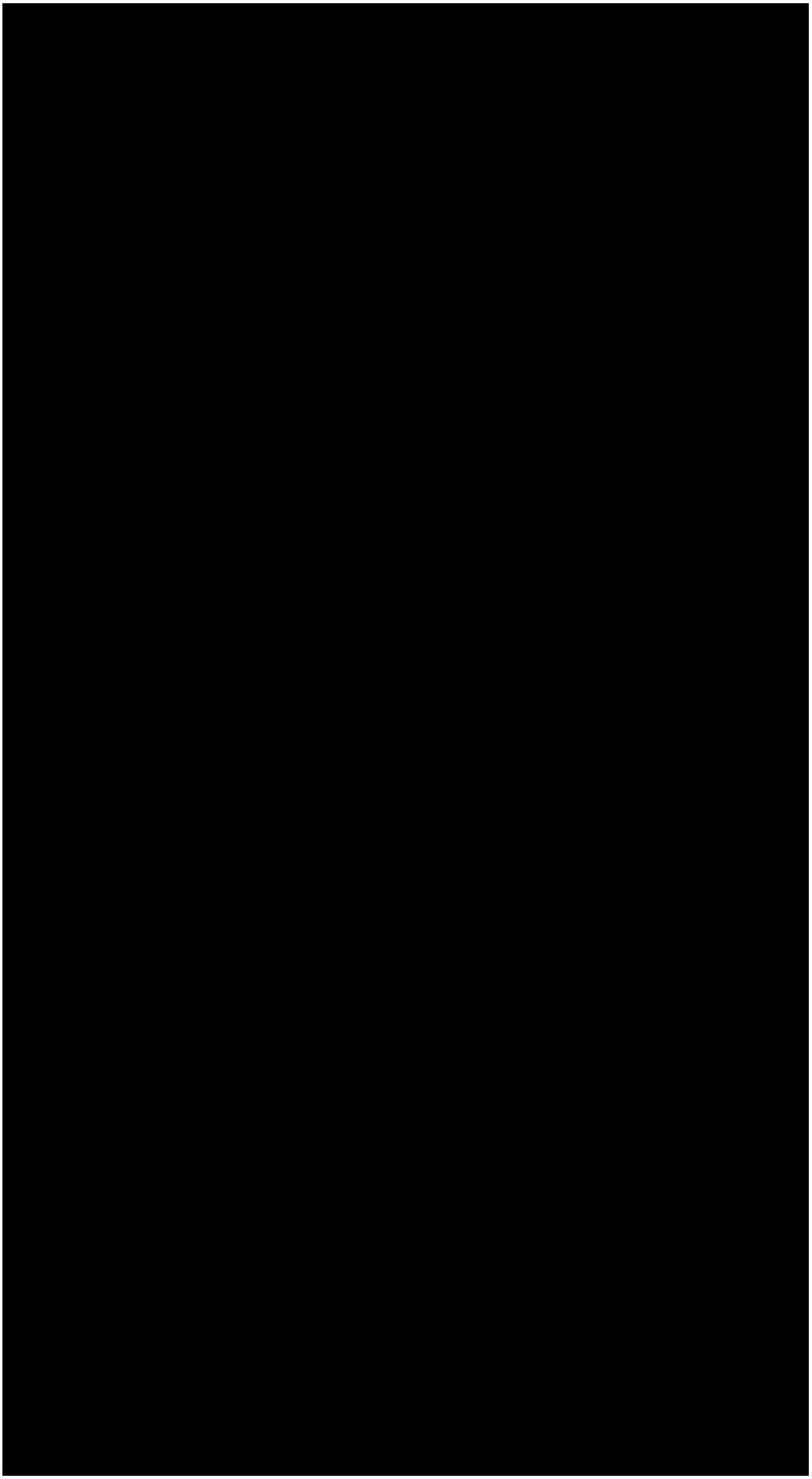
Cybersecurity at GM

40. GM takes seriously the secure design, implementation, and maintenance of vehicle systems and vehicle data. As part of vehicle design, GM has developed a comprehensive system of cybersecurity controls to provide layers of protection against cyber threats, consistent with NHTSA's guidance. GM follows what it terms a defense-in-depth approach to cybersecurity.

41. Under this approach, GM layers several security controls to protect vehicle systems and data. At the center of it all is GM's secured or central gateway, that keeps functions segregated

and thus less vulnerable to cyber threats. If one security control is compromised, an attacker is confronted by another security control to thwart an attack. This multi-layered approach with intentional redundancies increases holistic security.

42. Methods GM uses to secure its vehicle systems include using challenge and response protocols, unique identifiers, rationality checks to control the availability and execution of safety and security-critical diagnostic routines, secure storage controls to safeguard sensitive personal and vehicle information, in-vehicle network message authentication, password protections, logical and physical isolation, firewalls designed to control and protect the flow of messages among vehicle systems, network domain segregation, intrusion detection and prevention systems, encryption keys, software authenticity and integrity checks to safeguard vehicle component firmware programming and bootloader execution, and secure communication channels between onboard vehicle systems and offboard computer servers. What follows on the next page is a graphical representation of the various controls GM deploys and the ways in which they are layered on top of each other. *See* Chart entitled GM Product Cybersecurity Defense-in-Depth (AAI-GM-0000035), a true and correct copy of which is attached hereto as Trial Exhibit 16.



Challenge and Response Protocols

43. GM uses an access control commonly referred to as a challenge and response protocol as an element of design of safety-critical and emissions ECUs.

44. [redacted]

45. [redacted]

46. The challenge and response protocols ensure that threat actors cannot tamper with safety-critical functions while making software changes to safety-critical ECUs. [redacted] Attached hereto as Trial Exhibit 53 is a true and correct copy of a presentation entitled *Secure Diagnostics & Secure Unlock* (AAI-GM-

0000187). That presentation describes the secure access challenge and response process used for diagnostics. That presentation was prepared in October 2019 and is maintained in GM's technical repository, which is a repository of product cybersecurity technical documents regarding GM's vehicle systems.

Rationality Checks

47. "Rationalizing" by way of rationality checks is the process of assessing the condition of the vehicle before the service technician can deploy a diagnostic.

48. [redacted] *See* Trial Exhibit 53 (AAI-GM-0000187).

49. [redacted]

50. [redacted]. Those redundant layers work to prevent breaches that could endanger the safe operation of safety-critical functions regulated by the FMVSS and that are otherwise necessary for the safe operation of GM vehicles.

Message Authentication

51. [redacted]

[redacted]

52. Message authentication bolsters the security surrounding the interfaces that facilitate communications between vehicle components. For the vehicle to operate, the various components must interface with one another. Additionally, certain components must communicate to external devices, such as diagnostic tools.

53. The possibility that these communications by and between vehicle components may be intercepted or altered is a grave safety risk. For example, the manipulation of a message to the transmission control unit might trigger a vehicle to uncontrollably accelerate.

54. [redacted] Attached hereto as Trial Exhibit 40 is a true and correct copy of the presentation entitled *Product Cybersecurity – Message Authentication Overview* (AAI-GM-0000013), which provides an overview of message authentication. That presentation was prepared by me and my team in March 2016.

55. Message authentication prevents threat actors from sending unauthorized messages to a vehicle's safety-critical ECUs.

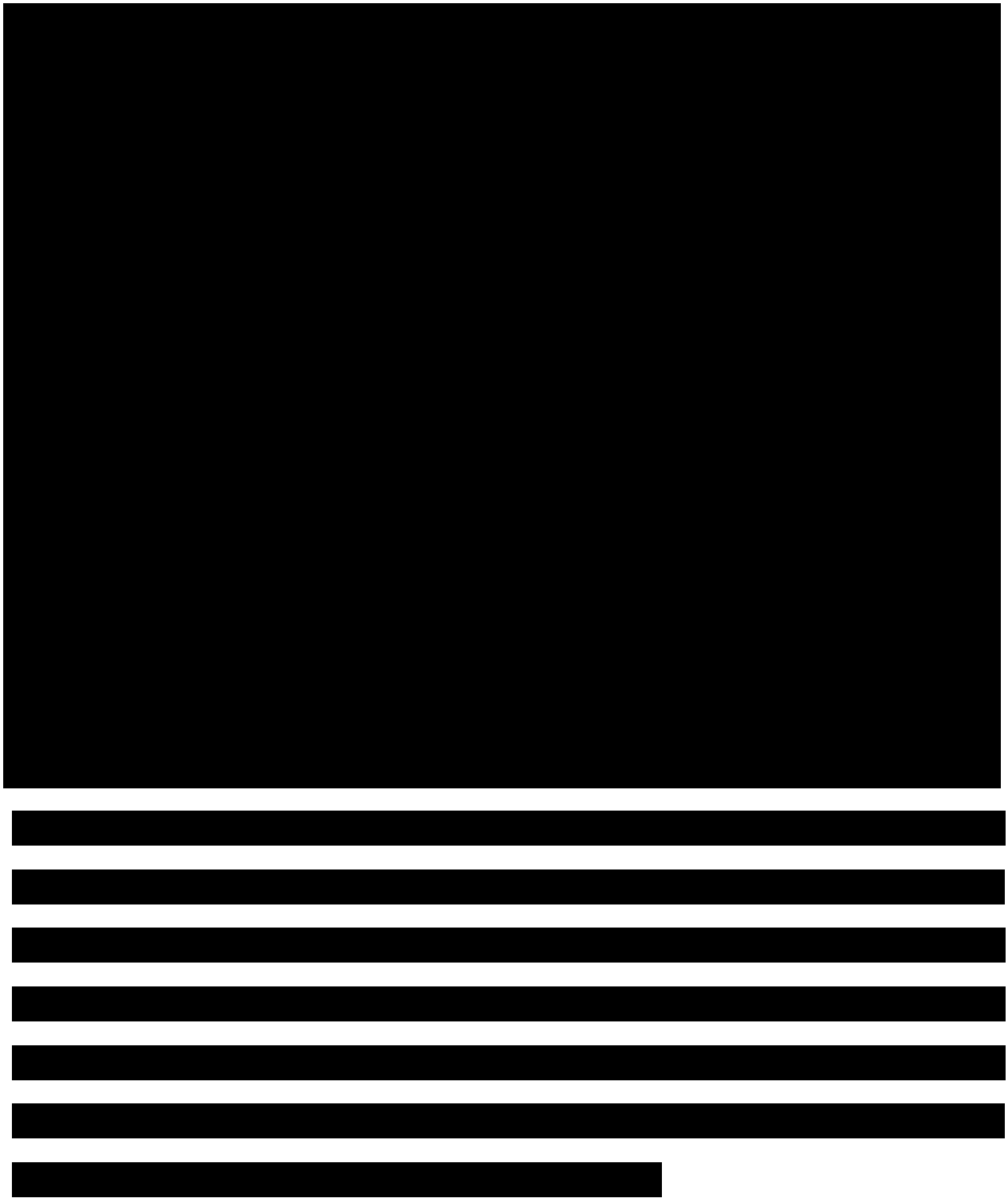
56. [redacted]

[redacted]

Logical and Physical Isolation

57. GM uses both logical isolation and physical isolation to provide layers of protection against cybersecurity threats. Logical isolation means that control units that share the same physical network infrastructure nevertheless do not communicate directly with one another. Physical isolation is where a control unit has two or more real processors dedicated to distinct functions, such as telematics and network communications, as opposed to combining their functions in one processor. Through a combination of these two techniques, GM helps to ensure that safety-critical functions are isolated from other vehicle features—meaning, for instance, that malware introduced to a vehicle's radio system is far less likely to affect a vehicle's steering.

58. [redacted] *See* Presentation entitled *Electrical Architecture: Driving Security Controls in Global A and Global B* (AAI-GM-0001567), a true and correct copy of which is attached hereto as Trial Exhibit 41. This presentation was created by my team at GM in September 2019. [redacted]



Firewalls

59. As part of the isolation structure, a system of firewalls in the secure gateway limits the flow of messages between vehicles systems. Firewalls scan network traffic and block

potentially harmful messages, allowing firewalls to keep out viruses and threat actors. [redacted]

60. [redacted] *See* Presentation entitled *Cybersecurity Strategy – Global A* (AAI-GM-0000002), which was prepared by me in 2014, and a true and correct copy of which is attached hereto as Trial Exhibit 52. [redacted]

[redacted]

[redacted]

61. Removing these firewalls would expose safety-critical systems and increase the risk of compromise of these systems. [redacted]

Intrusion Detection and Prevention Systems

62. Intrusion detection and prevention systems are a rapidly evolving technology that allows GM vehicles to monitor traffic on their internal networks and identify malicious activity. [redacted]

[redacted]

63. [redacted]

64. [redacted] This provides isolation between the connected side of the vehicle, including radio and telematics control units and networks, and the safety-critical side of the vehicle, including acceleration, steering, braking, and airbag control units and networks.

Encryption

65. [redacted]

Encryption employs an algorithm to transform the data to make it inaccessible without the key or underlying algorithm. Encryption helps to prevent a threat actor from accessing and using the data.

Firmware Safeguards

66. Firmware is the software encoded onto a vehicle's ECUs. For ECUs governing core vehicle safety functions firmware executes core vehicle safety functions related to steering,

acceleration, braking, and airbags. Tampering with the vehicle's firmware impacts these vehicle functions.

67. As part of its defense-in-depth strategy, GM relies on multiple safeguards to ensure the integrity of vehicle firmware. Two key mechanisms are digital signatures and secure boot, both employing asymmetric cryptography. *See* Presentation entitled *Secure Programming and Secure Boot: Safeguarding Vehicle Software* (AAI-GM-0000201), which was prepared by my team at GM, and a true and correct copy of which is attached hereto as Trial Exhibit 43.

68. [redacted]

69. [redacted]

70. [redacted]

71. The security of the public and private key structure is inextricably dependent on GM. This public key infrastructure (PKI) is fundamental to the security and safety of GM's customers, and GM goes to great lengths to protect the security and integrity of these systems.

[redacted] The security of the PKI would be more likely to be compromised if held on a less secure system, defeating the purpose of this security protocol and would give threat actors another potential access point to exploit. Moreover, a purpose of the security keys is to ensure verified, safe GM firmware is on the vehicle. Opening the keys to third parties would negate this purpose, as third parties could use the private key to install un-vetted, third-party firmware altering safety-critical ECUs and endangering consumers.

72. The secure boot process also protects the integrity of the firmware. [redacted]

Secured Communication Channels

73. Secured communication channels protect communications between the vehicle, GM, and the consumer. Using Transport Layer Security (TLS), the communications are encrypted while in transit and require certification on all ends.

74. GM's mobile application is an example of the use of secured communication channels. At this time, GM's mobile application only has limited features and messages that can be sent to the vehicle, such as locking or unlocking a vehicle, turning the vehicle on or off, and checking tire pressure. The application does not allow for commands to safety-critical functions

such as braking systems. [redacted]

75. The security of the mobile application is currently dependent on GM's role in receiving and validating requests from the application before conveying the message to the vehicle. [redacted]

76. OnStar, GM's telematics system, also relies on secured communication channels. [redacted] *See* Presentation entitled *OnStar Telematics Network Security Architecture* (AAI-GM-0001687), a true and correct copy of which is attached hereto as Trial Exhibit 12.

77. Wider access to the encryption key for the secured communication channel would undermine the security of the key. If just one party with access to the key is compromised, the key could be available to threat actors to intercept and manipulate communications to and from the vehicle. GM believes that the manufacturer remains the party best able to protect encryption keys for its vehicles, because it alone has full knowledge of its vehicle systems and their capabilities as well as the ability to validate and certify any software changes. Manufacturers are also uniquely

motivated to ensuring adequate cybersecurity protection, to protect their customers and brand image from harm due to breach.

Data Law Compliance

78. GM complies with all laws related to vehicle data access, including the predecessor Massachusetts "Right to Repair" law. Accordingly, GM currently makes available for purchase by all owners and independent repair facilities the same data necessary to diagnose, repair, or maintain GM vehicles that it provides for purchase to GM dealerships. In addition to data, GM also makes available to owners and independent repair shops diagnostic tools with the same diagnostic capabilities as the tools used by GM dealerships.

79. At the same time, GM does not make all vehicle data and systems accessible to anyone—whether a dealership, an independent repair shop, or a vehicle owner. Doing so would be antithetical to GM's defense in depth cybersecurity approach, and to federal law that contemplates maintaining sufficient cybersecurity protections around safety- and emissions-critical functions.

80. The Data Law upends this approach by mandating broad access to a nearly limitless volume of vehicle data, the creation of novel standardized platforms for access to that data, and all on a grossly unrealistic timeline for compliance.

81. I wholeheartedly agree with NHTSA's assessment of the Data Law's requirements. *See* NHTSA Testimony to Massachusetts Legislature. Attached hereto as Trial Exhibit 60 is a true and correct copy of NHTSA's Testimony to Massachusetts Legislature. Back when the ballot initiative that eventually became the Data Law was under consideration by the Massachusetts Legislature, NHTSA concluded that manufacturers would have to "redesign their vehicles in a

manner that necessarily introduces cybersecurity risks, and to do so in a timeframe that makes design, proof, and implementation of any meaningful countermeasure effectively impossible." *Id.*

82. Indeed, in an attempt to comply with the Data Law, GM would have to remove the layered cybersecurity controls it designed and installed in vehicle electrical systems to protect safety- and emissions-critical functions. Doing so is inconsistent with GM's federal law obligations.

83. My understanding of Section 2 of the Data Law is that it requires manufacturers to do one of two things. Either they must give vehicle owners and independent repair facilities access to vehicle OBD systems that is "standardized" and that does not require "any authorization by the manufacturer, directly or indirectly." Data Law § 2. Or they must ensure that the authorization system for access to "vehicle networks and their [OBD] systems is standardized across all makes and models sold in the Commonwealth and administered by an entity unaffiliated with the manufacturer." *Id.*

84. Either way, then, Section 2 cuts the manufacturer out of the authorization and authentication process for access to OBD systems.

85. I am unaware of any currently existing system architecture that would allow standardized access to all aspects of OBD systems that does not require any authorization by the manufacturer, directly or indirectly. I am also unaware of any currently existing system architecture that would allow access to "vehicle networks" and OBD systems that is administered by a third-party unaffiliated with a manufacturer.

86. Indeed, the Data Law's reference to "vehicle networks" would seem to include every electronic networked component of the vehicle—encompassing components far beyond anything even remotely related to vehicle diagnosis, repair, or maintenance.

87. For vehicles with telematics systems, Section 3 of the Data Law requires that manufacturers provide an "inter-operable, standardized and open access" platform that is (1) capable of securely communicating all mechanical data—defined separately in the law to include all data "otherwise related to vehicle diagnosis, maintenance and repair," including "telematics data"—via direct connection to the platform; (2) directly accessible by the vehicle owner through a mobile-based application; (3) directly accessible by independent repair facilities; and (4) provides independent repair facilities with the ability to send commands to in-vehicle components.

88. I am unaware of any currently existing platform that would allow for "inter-operable, standardized and open access" to all vehicle data otherwise related to vehicle diagnosis, repair, or maintenance—let alone one that is standardized across all makes and models, either within a manufacturer or across the industry.

89. GM employs the cybersecurity controls discussed to protect things like acceleration, braking, steering, and airbags, and to ensure that those functions operate as required by federal law.

90. Sections 2 and 3 of the Data Law would require GM to remove key cybersecurity controls that it installed in vehicles as parts of the element of design around safety- (and emissions-) critical functions. That is because the requirements in Sections 2 and 3 of the Data Law run counter to the cybersecurity approaches GM uses to help ensure that safety- (and emissions-) critical functions on vehicles are protected from threat actors or even owners themselves who might inadvertently introduce malware.

91. The Data Law's mandate for standardization across vehicle makes and models is contrary to GM's approach to protecting vehicle networks. The standardization the Data Law requires is problematic from a cybersecurity perspective because it removes diversity within and

between the vehicle systems covered by the law. Because access would be standardized across vehicle makes and models, if a threat actor were able to gain access to one vehicle system, he could then access all vehicles—significantly magnifying the scale of any attack.

92. GM understands well the benefits of a security-by-diversity model to prevent large scale attacks. Security by diversity is the practice of simultaneously using different systems across different products. Even within the GM fleet, then, GM vehicles use different versions of ECUs and different mechanisms for establishing trust and security credentials. The differences among these vehicles increases the bar for a threat actor to perpetrate a mass attack. Standardization across the entire automotive industry would create an enormous attack surface for any threat actor attack or malware introduced into a vehicle. With standardized access, what might be an isolated event affecting very few vehicles could immobilize vehicles across all manufacturers.

93. The Data Law's access requirements without manufacturer authorization further implicates GM's protections surrounding sensitive firmware. GM vehicles are designed to permit firmware changes only when GM digitally signs the software update. GM maintains these highly-sensitive, private keys on its secure servers. To comply with the law, GM would have to make these private keys public to provide the requisite access while removing GM from the process.

94. If manufacturers are not involved in the authorization process, then they cannot prevent third parties from changing vehicle data. This poses an unnecessary and unacceptable risk that threat actors, or even unsuspecting drivers or technicians, would introduce malicious software or install emissions defeat devices. This faulty software could be extremely dangerous if it disabled power steering or caused a vehicle's brakes to malfunction.

95. The concept of access to all "vehicle networks" or "open access" platform runs counter to all notions of cybersecurity protections. In addition to the risks associated with

standardization, open access would allow third parties to manipulate sensitive vehicle systems without the manufacturer's security protections. Third parties would be able to read, modify, and write new data to vehicles, increasing the risk to unauthorized modification of safety-critical features like acceleration, braking, and steering.

96. Allowing "open access" to vehicle systems without manufacturer authorization would compromise the integrity of vehicle systems and the safe operation of vehicles. It would greatly increase the severity of any cybersecurity attacks by giving third parties who access those systems greater ability to compromise the vehicle intentionally or unintentionally.

97. To implement the required access, GM would have to abandon layers of security controls around its safety and emissions related vehicle systems—including challenge and response protocols, authenticated security keys, firewalls, and the logical and physical isolation ensured by the vehicle's secured gateway. Threat actors would have free rein to compromise vehicle safety and emissions performance.

98. GM relies on a defense-in-depth security strategy with layers of purposeful redundancy. GM has purposely built these protections into the design of the systems to ensure the safety of its vehicles. Removing key parts of that strategy would degrade cybersecurity controls.

99. Under the Data Law, GM would have to remove the following specific safety-critical cybersecurity controls to provide the broad data access required by Sections 2 and 3: (i) firewalls and gateways that prevent unauthorized messages from reaching safety-related ECUs; (ii) access controls, including the challenge and response protocol as well as message authentication, (iii) firmware safeguards, and (iv) secured communication channels.

100. To take one example, GM would have to abandon the current cybersecurity approach that segregates certain safety- and emissions-critical ECUs from others to provide access

to all "vehicle networks" (Data Law § 2) or provide "open access" to a wide array of vehicle data "otherwise related to" maintenance, diagnosis or repair, *id.* § 3. [redacted]

[redacted] *See* Trial Exhibit 41.

[redacted]

Under the Data Law's broad access regime, however, GM could not maintain this separation. The Data Law's conception of mechanical data would crosscut the existing, segregated CANs.

101. This would be a momentous change that would seriously compromise vehicle safety and emissions. The central gateway is critical to segmenting more vulnerable, connected features such as telematics from emissions ECUs and safety-critical ECUs that control acceleration, steering and ABS, braking, and crash protections such as airbags. Removing this

segmentation would mean that if a threat actor or malware made its way into a vehicle, it could affect all ECUs including those controlling safety and emissions functions. And removing the gateway would also necessarily mean removing firewalls built into the gateway.

102. GM also could no longer use its secured communication channels that prevent tampering with the messages sent to or from the vehicle. The current configuration of these channels depends on GM managing and securing the communications with encryption keys held by GM.

103. Moreover, communications from GM's mobile application are designed to be communicated to GM's server for authentication before GM sends a message to the vehicle. The Data Law forbids GM from serving as a conduit between the mobile application and the vehicle. By vetting messages from the mobile application, GM is able to identify potentially malicious messages before they reach the vehicle. Removing GM from the communication flow without an adequate replacement would immediately expose vehicles to significant risks from threat actors who gain access to a driver's phone.

104. The lack of secure communication channels coupled with the Data Law's requirement that third parties be able to read and write new data to the vehicle is perilous. Allowing third parties to have this access would allow threat actors to take control of vehicles remotely, giving them control over a vehicle's brakes, steering, or acceleration. Even under its current design, GM does not support use of its mobile application to read and write new data to the vehicle. The mobile application's capabilities are limited to the transfer of certain diagnostic codes and the deployment of a few commands—for example, remote start. Use of the existing mobile application infrastructure to comply with the Data Law is not feasible.

105. Moreover, GM's current cybersecurity controls limit the capabilities of the GM mobile application. GM does not allow the mobile application to directly write software to the vehicle. By design, telematics are separated from safety and emissions related components. Because the Data Law requires the ability for a mobile application to send commands to these ECUs, GM would have to remove the firewalls and central gateway module designed to isolate telematics from safety- and emissions-critical ECUs.

106. And GM would have to disable the challenge and response protocols and message authentication requirements that prevent unauthorized communications to the ECUs. Those protocols currently block certain commands from the telematics system to ECUs for safety-critical functions. But since the Data Law requires "open access" to any data "otherwise related to the diagnosis, repair or maintenance of the vehicle," including telematics data, Data Law §§ 1, 3—that is to say, unlimited read-write access to nearly all vehicle components—GM would have to remove those access controls.

107. The "solutions" I have heard suggested by the Attorney General would not resolve the fundamental cybersecurity problems with the Data Law. The Attorney General has proposed two—(1) having a third party (other than the manufacturer) control access to vehicle electronic architecture through a public key infrastructure ("PKI") and (2) disable telematics systems. Neither addresses the fundamental issues with the Data Law, and both would introduce security risks.

108. Having a third party control access to all keys is not a secure solution. The many layers of cybersecurity protections that GM employs in its vehicles are far too complex simply to transfer to a third party, much less one for the entire automotive industry. And the precise security controls vary among vehicles. [redacted]

[redacted] Even if a third party could theoretically manage access keys, the Data Law would remove a manufacturer's ability to exercise control over this third party—because the manufacturer could not be involved in authorization decisions "directly or indirectly" or the third party must be "unaffiliated with the manufacturer." Data Law § 2. At the same time, manufacturers would continue to carry the obligations to comply with federal law and would suffer any negative repercussions to brand image from major safety issues, recalls, or civil liability. Third parties simply do not have the same incentives to keep vehicles secure.

109. Moreover, the mere act of adding an unaccountable third party to serve as a middleman between the manufacturer and the consumer increases safety risks. This new third party would give threat actors a new target for potentially accessing vehicles. This is especially true given that manufacturers would have no control over third parties to ensure that they use appropriate cybersecurity protocols. The use of standard software would make it more difficult to trace any breach that does occur because there will be nothing unique about the software to identify the source of the breach.

110. Manufacturers also manage a wide range of updates being made across the entire fleet of vehicles at any given time. These updates require coordination to reach as many drivers as possible. Manufacturers are also uniquely well-situated to design software to fix safety issues because they are the most familiar with vehicle systems and performance and can best test and certify new software. That is why, now, in accordance with NHTSA's guidance, manufacturers are involved in any updates to vehicle firmware.

111. Disabling telematics is not a viable solution to the requirements in Section 3 of the Data Law. The vast majority of vehicles GM makes available for purchase to individual consumers include telematics systems. It is a practical impossibility to disable telematics systems for all vehicles that might one day be resold in the Massachusetts aftermarket. Doing so immediately also defies reality where contracts with dealerships and customers contemplate the continued use of those systems.

112. There is a reason why modern vehicles use telematics—and not all of them are related merely to driver convenience. Disabling telematics would make recalls, including recalls for emissions and safety-critical issues, slower and less effective and would remove emergency crash notifications, which automatically sends a message to emergency personnel that there has been an accident. These vehicles without telematics systems would then necessarily make their way to other states through second-hand car sales in the aftermarket, amplifying the Data Law's effects throughout the country.

113. The safety and cybersecurity risks entailed by the Data Law would have a devastating impact on the safety of Massachusetts citizens, as well as GM. Massachusetts drivers' vehicles would be less safe and more susceptible to hacking by a threat actor or potentially disastrous problems caused by even a well-intentioned novice attempting to tinker with complicated electronic vehicles systems . GM's reputation as a leading auto manufacturer, in turn, depends on its long track-record of offering consumers safe and reliable vehicles, and any increased potential for cybersecurity attack risks damaging that reputation.

114. Also attached to this affidavit are true and correct copies of the following Trial Exhibits, which were produced from GM's records:

- Trial Exhibit 2 (Bates number AAI-GM-0000008), which is a 2015 presentation entitled Vehicle & Vehicle Services Cybersecurity DLC Protection for Global A.
- Trial Exhibit 5 (Bates number AAI-GM-0000030-32), which is the April 1, 2018 GM Data Link Connector Policy.
- Trial Exhibit 6 (Bates number AAI-GM-0001192), which is a July 2019 presentation entitled Global Cybersecurity: NHTSA Meeting.
- Trial Exhibit 7 (Bates number AAI-GM-0001422-1511), which are CAN Bus topology documents.
- Trial Exhibit 11 (Bates number AAI-GM-0001585-1617), which is the Global A Topology Version 7.4.3.
- Trial Exhibit 17 (Bates number AAI-GM-0000029), which is a March 17, 2018 GM Policy on 3rd Party Aftermarket DLC Devices.
- Trial Exhibit 42 (Bates number AAI-GM-0000028), which is a November 20, 2017 Product Cybersecurity Overview presentation that was prepared by me and other GM employees for the GM Cybersecurity Risk Committee.
- Trial Exhibit 44 (Bates number AAI-GM-0000014-16), which are GM Vehicle Cybersecurity Guidelines dated January 28, 2016. These guidelines were prepared by GM's cybersecurity team and reviewed by me.
- Trial Exhibit 45 (Bates number AAI-GM-0000012), which is a GM presentation regarding vehicle data control points prepared by me and my team in 2016.
- Trial Exhibit 46 (Bates number AAI-GM-0000053), which is a chart entitled Data Access & Device Support for Data Link Connector (DLC/OBDII) Port – GM Electrical

Architecture. I am well-familiar with this document, which was prepared by GM employees in March 2019 and which I have reviewed in my regular course of work.

- Trial Exhibit 54 (Bates number AAI-GM-0000190), which is a presentation entitled Global B Electrical Architecture Overview. That presentation is maintained in GM's technical repository, which is a repository of technical documents regarding GM's vehicle systems.
- Trial Exhibit 55 (Bates number AAI-GM-0001512-41), which are vehicle network diagrams prepared in 2019 by GM.
- Trial Exhibit 75 (Bates number AAI-GM-0000025), which is a 2016 presentation I gave entitled "Product Cybersecurity: 101."
- Trial Exhibit 76 (Bates number AAI-GM 0000038), which is a November 2018 presentation I gave entitled "Global B Risk Assessment – Cybersecurity."
- Trial Exhibit 77 (Bates number AAI-GM-0000019), which are 2016 slides regarding GM connected vehicle attack surfaces and connected vehicle ecosystems.
- Trial Exhibit 78 (Bates number AAI-GM-0000026), which is a March 2017 presentation entitled "General Motors Product Cybersecurity NHTSA Overview."
- Trial Exhibit 79 (Bates number AAI-GM-0000052), which is a 2019 slide entitled "Electrical Architecture Cybersecurity Capability vs. Lifecycle."
- Trial Exhibit 56 (Bates number AAI-GM-0000009), which is a GM policy entitled Vehicle Cybersecurity.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on: June 10, 2021

/s/ *Kevin Tierney*
Kevin Tierney